EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

A.M. and J.K., *individually and on behalf of all others similarly situated*, Plaintiffs, v. ADVANCED REPRODUCTIVE HEALTH CENTER, LTD. d/b/a CHICAGO IVF, Defendant.	**Case No. 1:24-cv-07559** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs A.M. and J.K. (collectively, "Plaintiffs") bring this class action lawsuit, individually and on behalf of all others similarly situated (the "Class Members"), against Advanced Reproductive Health Center, Ltd. d/b/a Chicago IVF ("Defendant"). The allegations set forth herein are based on Plaintiffs' personal knowledge and on information and good faith belief as to all other matters based upon investigation by counsel.

INTRODUCTION

1. Fertility treatment can be a difficult journey—both physically and emotionally. One in eight couples has trouble getting pregnant or carrying a pregnancy, and 7.4 million women have received infertility treatment.[1] Despite the prevalence of infertility, information concerning fertility and reproductive health is among the most confidential and sensitive information in our

[1] *See How to Support Someone Experiencing Infertility*, https://www.nm.org/healthbeat/healthy-tips/emotional-health/How-to-Support-Someone-Experiencing-Infertility (last visited Feb. 28, 2024).

society. According to a recent study, most infertile women choose to keep their struggle private from family or friends.[2]

2. Regarding the need to keep information about reproductive health private, the Department of Health and Human Services ("HHS") has noted:

> A positive, trusting relationship between individuals and their health care providers is essential to an individual's health and well-being. The prospect of releasing highly sensitive PHI can result in medical mistrust and the deterioration of the confidential, safe environment that is necessary to quality health care, a functional health care system, and the public's health generally. That is even more true in the context of reproductive health care, given the potential for stigmatization and other adverse consequences to individuals resulting from disclosures they do not want or expect.[3]

3. The mishandling of such private and sensitive health information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[4] Simply put, if people do not trust that their sensitive private information will be kept private and secure, they may be less likely to seek medical and fertility treatment which can lead to much more serious health consequences down the road. In addition, protecting

---

[2] *See What to Say to Someone Struggling With Infertility*, https://www.nytimes.com/2020/04/17/parenting/support-friend-infertility.html (last visited Feb. 28, 2024).

[3] *See HIPAA Privacy Rule To Support Reproductive Health Care Privacy*, https://www.federalregister.gov/documents/2023/04/17/2023-07517/hipaa-privacy-rule-to-support-reproductive-health-care-privacy (last visited Feb. 28, 2024).

[4] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."), https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Feb. 28, 2024).

medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

4. Defendant Chicago IVF provides fertility treatment to couples seeking to start a family.[5] Defendant has locations throughout the Chicagoland area and provides treatments such as artificial insemination, in vitro fertilization, and genetic testing.[6]

5. As part of the medical services it provides, Chicago IVF owns, controls and maintains a website for its clinic, https://www.chicagoivf.com (the "Website").

6. Defendant Chicago IVF actively encourages patients and prospective patients to use the Website, to communicate with their healthcare providers; manage medical appointments for fertility services; search medical conditions concerning fertility conditions and treatment options. The Website invites patients to share and search for personal medical information about their own reproductive health. And patients, trusting that this extremely private and sensitive information will be safeguarded, share intimate and personal medical information with Chicago IVF through the Website.

7. Defendant knows that its patients expect the intimate details of their treatment to remain confidential. In an effort to reassure its patients that their information is protected, Chicago IVF proclaims to its patients in its "Privacy Policy" that "[w]e want you to understand that we respect your privacy. Other than the necessary uses and disclosures we described above, we will not sell your health information *or provide any of your health information to any outside marketing company*."[7] But Defendant does not live up to its promises.

---

[5] *See* https://www.chicagoivf.com/about (last visited Aug. 15, 2024).

[6] *Id*.

[7] *Privacy Policy*, https://www.chicagoivf.com/privacy-policy (emphasis added) (last visited Aug. 15, 2024).

8. Unbeknownst to Plaintiffs and Class Members, Defendant installed tracking technologies, including, but not limited to, the Meta Pixel (the "Pixel"), Google Analytics, and Google Tag Manager, (collectively, "Tracking Technologies")[8] on its Website to collect and disclose its Private Information to unauthorized third parties for its own pecuniary gain. The collection and transmission of this information is instantaneous, invisible and occurs without any notice to—and certainly no consent from—the Users.

9. The Meta Pixel, installed and configured by Defendant, is a piece of code that "tracks the people and [the] type of actions they take"[9] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

10. The Pixels—which are configured by the website owners, here, Chicago IVF—collect and transmit information from Users' browsers to unauthorized third parties, including, but not limited to, Facebook.[10]

---

[8] This Complaint contains images and evidence demonstrating the Meta Pixel was used on Defendant's Website, but Plaintiffs (without the benefit of discovery) do not have access to every tracking tool that was previously installed on the Website.

[9] *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Feb. 28, 2023).

[10] The pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the pixel to a webpage is a multi-step process that, as described in detail in *Section E*, must be undertaken by the website owner such as Chicago IVF.

While this Complaint primarily focuses on how Defendant embedded the Meta Pixel on their Websites to collect and disclose Users' Private Information, other secret tracking technologies embedded by Defendant—such as for example Google Analytics tracking codes—also collect such Private Information, and the respective tech companies have the capability to link it to specific user profiles.

11. Together with the patients' Private Information, the data sent to Facebook also discloses Users' unique and persistent Facebook ID ("Facebook ID" or "FID") which allows Facebook and other third parties to personally identify those Users and associates their Private Information with their Facebook profile.[11]

12. Simply put (and as detailed herein), healthcare providers such as Defendant are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent from each patient. Neither Plaintiffs nor any other Class Members were provided—much less signed—a written authorization permitting Defendant to disclose their Private Information to Facebook or any other third-party data brokers.

13. Plaintiffs and Class Members who visited and used Chicago IVF's Website ("Users") reasonably believed that they were communicating only with their trusted healthcare providers.

14. At no point has Defendant, despite intentionally incorporating invisible tracking code from unauthorized third parties into its Website, informed Users that their personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to

[11] The Facebook ID is a unique string of numbers Facebook uses to identify and connect to a User's Facebook profile via, among other methods, a *c_user* cookie. Facebook creates a Facebook ID automatically, whether or not you choose to create a username. Thus, Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it. *See Facebook Cookies Analysis*, https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a; *see also* https://www.cyberseo.net/blog/how-to-get-facebook-c_user-and-xs/ (last visited Feb. 26, 2024).

as "Private Information") communicated via its Website was intentionally disclosed to a third party—let alone Facebook,[12] which has a sordid history of privacy violations.[13]

15. As recognized by both the Federal Trade Commission ("FTC") and the Office for Civil Rights ("OCR") of HHS, healthcare companies' use of tracking technologies to collect and divulge their patients' sensitive and confidential information is an extremely serious data security and privacy issue:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***[14]

16. Similarly, the OCR is clear that "[r]egulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the Health Insurance Portability and Accountability Act ("HIPAA") Rules."[15]

---

[12] Meta Platforms, Inc. is doing business as "Meta" and "Facebook." The terms "Meta" and "Facebook" are used interchangeably throughout.

[13] This Court will not have to look far to find evidence of Meta's violations of privacy laws. Just in May of last year, for instance, the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last visited Feb. 28, 2024).

[14] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Feb. 28, 2024).

[15] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-

17. There is no anonymity in the information disclosed to Facebook; that is, the Pixel collects and discloses a substantial "data packet" coupled with the FID so that Defendant can, among other things, send targeted advertisements to Users based on their sensitive and protected Private Information. Defendant also uses this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use its Website.

18. Operating as designed and as implemented by Defendant, the Pixel disclosed information that allows a third party (*e.g.*, Facebook) to know when and where a specific patient was seeking confidential medical care, the medical condition(s) that patients inquired about, and the precise care the patient sought or received. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who target Plaintiffs' and Class Members' Facebook accounts based on that Private Information.

---

professionals/privacy/guidance/hipaa-online-tracking/index.htm (noting that "IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.").

This guidance was recently vacated *in part* by the Federal District Court for the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. *See American Hosp. Ass'n. v. Becerra*, No. 4:23-cv-01110-P, ECF No. 67 (S.D. Tex., Jun. 20, 2024). Notably, the court's order found only that the OCR's guidance regarding covered entities disclosing to third parties users' IP addresses while users navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id*. at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). Furthermore, the FTC bulletin on the same topics remains untouched, as do the FTC's enforcement actions against healthcare providers for committing the same actions alleged herein).

19. While the information captured and disclosed may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, the user's first name, last name, email address and phone number entered on the website. The data packets can also include the buttons a user clicks and the exact words a user types into a search bar.

20. The data in the "data packets" is then linked to the Users' Facebook ID.

21. For instance, when a User uses Defendant's Website where Tracking Technologies, such as the Meta Pixel are present, the Pixel transmits the contents of their communications to Facebook, including, but not limited to: (i) information about medical reproductive and fertility services and treatments; (ii) patient status; (iii) searches for specific doctors; (iv) the text of URLs visited by the User; (v) requests to make an appointment; and (vi) other information that qualifies as PII and PHI under federal and state laws.

22. By installing the Meta Pixel and other Tracking Technologies, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook (and other third-party data brokers).

23. The information intercepted by the Pixels and third-party tracking technologies is used to build incredibly fulsome and robust marketing profiles for individual Users and create targeted advertisements based on the medical conditions and other Private Information. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Chicago IVF chose to use the Pixel data for marketing purposes to bolster its revenue.

24. Simply put, Defendant put its desire for revenue over its patients' privacy rights.

25. As a healthcare provider, Defendant has certain duties and obligations to its patients. Defendant breached those duties and obligations in one or more of the following ways:

(i) failing to adequately review its marketing programs and web-based technology to ensure its Website were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web Users' information; (iii) failing to obtain the consent of Plaintiffs and Class Members to disclose their PII and PHI to Facebook or other third parties; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' PII and PHI through the Pixels; (v) failing to warn Plaintiffs and Class Members about the tracking technology present on the Website; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient PII and PHI.

26. Plaintiffs and Class Members have suffered injury because of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) compromise and disclosure of Private Information; (iv) diminution of value of their Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.[16]

27. Plaintiffs seek to remedy these harms for themselves and a class of all others similarly situated for: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*. (the "ECPA"), Unauthorized Interception, Use and Disclosure; (ii) Negligence; (iii) Unjust Enrichment; and (iv) Violation of the Illinois Eavesdropping Statute, 720 ILCS § 5/14-1, *et. seq*.

PARTIES

28. Plaintiff A.M. is, and has been at all relevant times, a resident of the city of Manhattan, Illinois.

[16] The exposed Private Information of Plaintiffs and Class Members can be—and likely has been—further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties often offer the unencrypted, unredacted Private Information for sale to criminals on the dark web for use in fraud and cyber-crimes.

29. Plaintiff J.K. is, and has been at all relevant times, a resident of the city of Plainfield in Will County, Illinois.

30. Defendant Chicago IVF is a corporation organized under the laws of Illinois with its principal place of business at 5225 Old Orchard Road, Suite 21, Skokie, in Cook County in the state of Illinois.

JURISDICTION & VENUE

31. This Court has federal subject matter jurisdiction pursuant to 28 U.S.C. § 1331 over the claims that arise under 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

32. This Court also has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

33. The Court has personal jurisdiction over Defendant Chicago IVF because its principal place of business and headquarters are located in Skokie, in Cook County, Illinois, it regularly engages in business in the State of Illinois and in Cook County and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this county.

34. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant that led to the unauthorized sharing of Plaintiffs' and Class Members' Private Information; Defendant's principal place of business is located in this District; Defendant collects

and redistributes Class Members' Private Information in this District and Defendant caused harm to Class Members residing in this District.

PLAINTIFFS' ALLEGATIONS

Plaintiff A.M.

35. Plaintiff A.M. accessed and used the Chicago IVF Website through her computer and mobile devices while located in Illinois to seek medical treatment as recently as July 2021.

36. Plaintiff A.M. attended her consultation and received services related to fertility treatment from Defendant.

37. Plaintiff A.M. used Defendant's Website to, among other things, search for a doctor, search for clinic locations, pay for medical services, schedule appointments, use the Patient Portal, and search for information regarding treatments and conditions for infertility, including for intrauterine insemination.

38. Information that Plaintiff A.M. provided to Defendant via its Website included queries about her medical conditions as well as for testing, diagnosis and treatments for intrauterine insemination.

Plaintiff J.K.

39. Plaintiff J.K. accessed and used the Chicago IVF Website through her computer and mobile devices while located in Illinois to seek medical treatment as recently as 2021.

40. Plaintiff J.K. has been a patient of Chicago IVF since approximately 2019 where she received in vitro fertilization treatment.

41. Plaintiff J.K. began using Defendant's Website in 2019 to, among other things, search for a doctor, search for clinic locations, pay for medical services, schedule appointments, use the Patient Portal, and search for information regarding treatments and conditions for

infertility, including in vitro fertilization treatments.

42. Information that Plaintiff J.K. provided to Defendant via its Website included queries about her medical conditions as well as for testing, diagnosis and treatments for in vitro fertilization.

43. Plaintiffs both maintained active Facebook accounts during the time they provided their Private Information to Defendant via its Website.

44. After Plaintiffs provided information to Defendant regarding their Personal Information, Plaintiffs both began receiving advertisements on their Meta accounts (Facebook and/or Instagram) for other fertility clinics that provide fertility treatment.

45. Plaintiffs reasonably expected that their communications with Defendant via the Website were confidential, solely between themselves and Defendant, and that such communications would not be transmitted to or intercepted by any third party without their full knowledge and informed consent.

46. Plaintiffs provided their Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

47. As described herein, Defendant worked along with Facebook to intercept Plaintiffs' communications, including those that contained confidential Private Information, while Plaintiffs were within the state of Illinois.

48. Defendant willfully facilitated these interceptions without Plaintiffs' knowledge, consent or express written authorization.

49. Within the State of Illinois, Defendant transmitted Plaintiffs' FID, computer IP address, location, information such as medical treatments and conditions, the scheduling of appointments, information on physician(s) she selected and her sensitive and private medical

information to Facebook.

50. The full scope of Defendant's interceptions and disclosures of Plaintiffs' communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiffs' past or present patient status, medical conditions (treatment for infertility and use of in vitro fertilization), treatments sought, and the locations for receipt of healthcare, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel and which contain information concerning Plaintiffs' specific medical conditions, queries, and treatments sought:

- https://www.chicagoivf.com/fertility-treatment/iui-artificial-insemination
- https://chicagoivf.securepayments.cardpointe.com/pay
- https://portal.chicago-ivf.com/PatientPortal
- https://www.chicagoivf.com/locations/fertility-clinics/naperville-western-chicago-suburbs
- https://www.chicagoivf.com/about/fertility-specialists/natalie-schultz-md

51. By doing so without their consent, Defendant breached Plaintiffs' right to privacy and unlawfully disclosed their Private Information.

52. Defendant did not inform Plaintiffs that it shared their Private Information with Facebook.

53. Plaintiffs suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of their Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) the continued and ongoing risk to her Private Information.

54. Plaintiffs have a continuing interest in ensuring that their Private Information is

protected and safeguarded from future unauthorized disclosure. Plaintiffs want to continue to communicate through online platforms but have no practical way of knowing if their communications are being intercepted and disclosed to Facebook, and thus continues to be at risk of harm from Defendant's conduct.

COMMON FACTUAL ALLEGATIONS

A. Defendant Installed and Configured Facebook Tracking Technologies on its Website.

55. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[17]

56. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

57. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications and servers, thereby enabling the interception and collection of website visitors' activity.

58. Specifically, the Pixel "tracks the people and type of actions they take."[18] When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers. Notably, this transmission does not occur unless the webpage contains the Pixel.

---

[17] *Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited May 23, 2024).

[18] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited May 23, 2024).

59. The Pixel is customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

60. The process of adding the Pixel to webpages is a multi-step process that must be undertaken by the website owner.[19]

61. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel: "(1) Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you, or you can manually add code to your website. (2) Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website."[20]

62. Aside from the various steps to embed and activate the Pixel, website owners, like Defendant, must also agree to Facebook's Business Tools Terms by which Facebook requires website owners using the Pixel to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook's Business Tools (including the Pixel) 29 and that websites "will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information . . . ."[21]

---

[19] Business Help Center: How to set up and install a Meta Pixel, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited June 1, 2024).

[20] *Id*.

[21] *Id.*; *see also* Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022) https://www.newsbytesapp.com/news/science/facebook-collects-personaldata-on-abortion-seekers/story (quoting Facebook spokesman Dale Hogan as saying that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people

63. Stated differently, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook but for Defendant's decisions to install the Pixel on its Website.

64. As explained in more detail below, this secret transmission to Facebook is initiated by Defendant's source code concurrently with Plaintiffs' and Class Members' communications to their intended recipient, Defendant.

B. Defendant Assisted Third Parties in Intercepting Patients' Communications with its Website and Disclosed Their Private Information to Third Parties.

65. Defendant's Website is accessible on mobile devices and desktop computers and allows patients to communicate with Defendant regarding their medical care.

66. Defendant encouraged patients to use its Website to communicate their Private Information, schedule appointments, access information about their treatments, pay medical bills and more.

67. Despite this, Defendant purposely installed Tracking Technologies on its Website and programmed specific webpage(s) to surreptitiously share its patients' private and protected communications, including Plaintiffs' and Class Members' PHI and/or PII, which was sent to Facebook, Google and other third parties.

68. The Tracking Technologies followed, recorded and disseminated patients' information as they navigated and communicated with Defendant via the Website, simultaneously transmitting the substance of those communications to unintended and undisclosed third parties.

69. The information disseminated by the Tracking Technologies and/or intercepted by third parties constitutes Private Information including medical information patients requested or viewed, the title of any buttons clicked (such as the "Services" drop down page which identifies and communicates the specific medical conditions and treatments of a patient), the exact phrases

---

through [its] Business Tools") (last visited June 1, 2024).

typed into text boxes, selections made from drop-down menus or while using filtering tools and other sensitive and confidential information, the divulgence of which is and was highly offensive to Plaintiffs.

70. This is PHI because the webpages have access to "information that relates to any individual's past, present, or future health, health care, or payment for health care."[22]

71. The information collected and disclosed by Defendant's Tracking Technologies is not anonymous and is viewed and categorized by the intercepting party on receipt.

72. The information Facebook received via the Tracking Technologies was linked and connected to patients' Facebook profiles (via their Facebook ID or "c_user id"), which includes other PII.

73. Similarly, Google stores users' logged-in identifier on non-Google websites in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses this data to serve personalized ads. [23]

74. Simply put, the health information that was disclosed via the Tracking Technologies is personally identifiable and was sent alongside other persistent unique identifiers such as the patients' IP address, Facebook ID and device identifiers.[24]

---

[22] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited June 20, 2024) (vacated by *American Hospital Association, et al. v Xavier Becerra, et al.*, No. 4:23-cv-01110-P, Dkt. No. 67 (N.D. Tex. June 20, 2024)).

[23] *See Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) (order denying summary judgment and citing internal evidence from Google employees).

[24] *See Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1056 (N.D. Cal. 2021) (discussing how Google

C. Defendant's Method of Transmitting Plaintiffs' & Class Members' Private Information via Tracking Technologies.

75. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (computer, tablet or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome, Mozilla's Firefox, Apple's Safari, and/or Microsoft's Edge browsers).

76. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' devices as their web browsers query the server through the internet.

77. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

1. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF to file a motion to a court.)

2. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

3. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.

---

collects personal information and IP addresses); *see also* https://developers.facebook.com/docs/meta-pixel/ (last visited May 23, 2024).

78. A patient's HTTP request essentially asks Defendant's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons and other features that appear on the participants' screens as they navigate Defendant's Website.

79. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

80. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP requests quietly executed in the background without notifying the web browser's user.

81. The Pixels are Source Code that do just that—they surreptitiously transmit a Website User's communications and inputs to the corresponding Pixel Information Recipient, much like a traditional wiretap.

82. For example, when individuals visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Pixels).

83. Thus, Defendant is, in essence, handing its patients a tapped website and, once a webpage is loaded into the patient's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications—intended only for Defendant—and instantaneously transmit those communications to Facebook or another corresponding Pixel Information Recipient

84. Third parties like Facebook place cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted

communication to ensure the third party can identify the specific user associated with the information intercepted (in this case, highly sensitive Private Information).

85. For example, Facebook uses cookies named c_user, datr, fr and fbp to identify Users. Facebook stores or updates Facebook-specific cookies every time a person accesses their Facebook account from the same web browser.

86. The Meta Pixel can access these cookies and send certain identifying information like the user's Facebook ID to Facebook along with the other data relating to the user's website inputs.

87. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

88. A User's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the User's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

89. The Facebook datr cookie identifies the User's web browser. It is an identifier unique to each person's specific web browser and is another way Facebook can identify Facebook users.

90. The Facebook fr cookie is a combination of the Facebook ID (c_user) and the browser ID (datr) cookie values.

91. A User who accessed Defendant's Website while logged into (or recently having logged into) Facebook would have their browser transmit the c_user, datr and fr cookies to Facebook.

92. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.

93. Defendant sent these identifiers with the Users' "event" data.

94. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with its Website (their IP addresses, Facebook ID, cookie identifiers, device identifiers, emails and phone numbers) and the "content" of these communications (the buttons, links, pages, and tabs they click and view related to their fertility-related health conditions and services sought from Defendant).

95. This disclosed PHI and PII allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with Defendant's ads, Facebook also then sells that information to marketers who will online target Plaintiffs and Class Members.

96. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiffs' and Class Members' status as medical patients;

b. Plaintiffs' and Class Members' communications with Defendant through its Website, including medical conditions for which they sought treatments and treatments sought;

c. Plaintiffs' and Class Members' searches for doctors;

d. Plaintiffs' and Class Members' contacting Defendant and making appointments for medical care; and

e. PII, including but not limited to patients' locations, IP addresses, device identifiers, individual's unique Facebook ID and other unique personal identifiers.

97. Through the Website, Defendant shares its patients' identities and online activity, including information and search results related to their private medical treatment.

98. For example, when they visit the Website, Chicago IVF patients can search fertility treatments by selecting the "Fertility Treatments" menu which takes them to a list of services offered by Chicago IVF. Patients are then directed to a variety of sensitive fertility treatments, including, for example "in-vitro-fertilization."

99. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries, without alerting the User, and the images below confirm that the communications Defendant Chicago IVF sends to Facebook contain the User's Private Information and personal identifiers, including but not limited to their Facebook ID, IP address, fbp, datr and fr cookies, along with the search filters the User selected.

100. Here, the search parameters set by the patient and the patient's FID number are being shared together, thereby allowing Facebook to make the direct connection between the search parameters and each individual patient's FID. Even without the FID, other identifying information like IP address or device identifier is captured by the Pixel and transmitted to Facebook. Facebook categorizes this event as a "PageView," which indicates that the patient viewed the webpage.

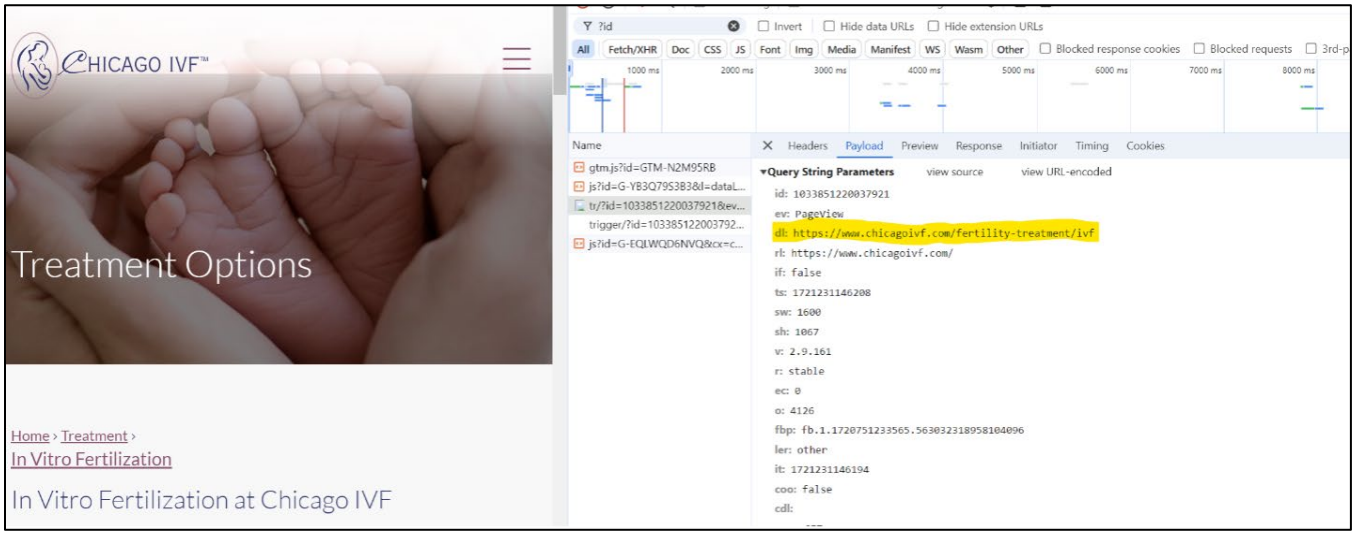
101. Every time Defendant sends a patient's Website activity data to Facebook, that patient's personally identifiable information is also disclosed, including their FID. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name.

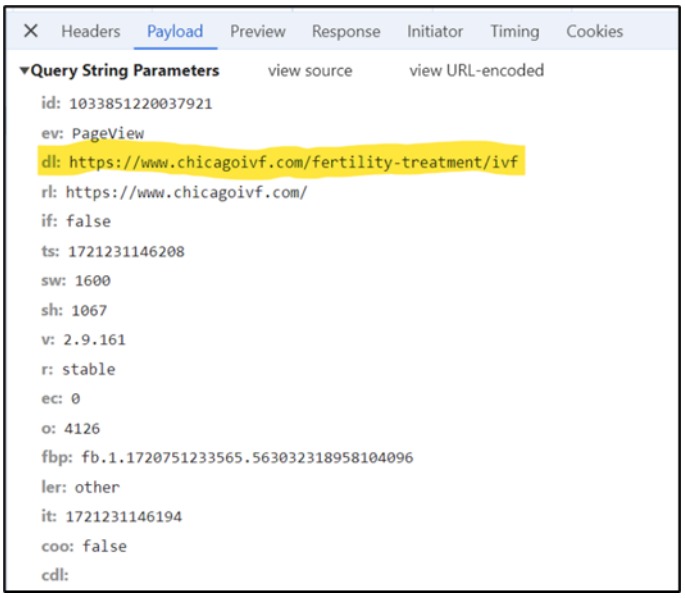
102. A user who accesses Defendant's Website while logged into Facebook will transmit

the c_user cookie to Facebook, which contains that user's unencrypted Facebook ID.

103. For example, a potential patient who is seeking in vitro fertilization treatment can choose the "Treatment" option on the Website that lists various options and then can click "In Vitro Fertilization."[25]

Figures 1 & 2: Examples of a HTTP single communication session sent from the User's device to Facebook that reveals the fact that the User is searching for "In Vitro Fertilization" treatment for infertility:





[25] *See* https://www.chicagoivf.com/fertility-treatment (last visited Feb. 28, 2024).

104. The first line of the highlighted text, "id:1033851220037921," refers to Defendant's Pixel ID for the Website and confirms that Defendant has downloaded the Pixel into its Source Code on this particular web page.

105. In the line of text below, "ev:" is an abbreviation for event, and "PageView" is the type of event. Here, this event means that Defendant's Pixel is sending information about the webpage being viewed, which can include information like page title, URL and page description.

106. The remaining lines of text identify the User as a patient: (i) seeking medical care from Defendant Chicago IVF via www.chicagoivf.com who is (ii) seeking "In Vitro Fertilization."

107. Defendant's Pixel sends the communications the user made via the webpage to Facebook, and the image below confirms that the communications Defendant sends to Facebook contain the user's personally identifiable information.

Figure 3: Example of a HTTP single communication session sent from the User's device to Facebook that reveals the User's unique personal identifiers including the FID (c_user field)

▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/? id=1033851220037921&ev=PageView&dl=https%3A%2F%2Fwww.chicagoivf.com &rl=https%3A%2F%2Fwww.chicagoivf.com&if=false&ts=1723003561598&sw=160 0&sh=1067&v=2.9.164&r=stable&ec=0&o=4124&fbp=fb.1.1722977900938.5555 77185344810325&pm=1&hrl=2bfc46&ler=other&it=1723003561543&coo=false &cs_cc=1&cs_cc=1&cas=7447779808673522%2C1587506458020758&cas=74477 79808673522%2C1587506458020758&cdl=&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9
Cookie:	sb=mGuDZrAj2tmZsAcbuWj2UQqD; datr=mGuDZpbJ8KwxccgYfgkn8yKV; c_user=61560564045991; xs=13%3AgJ4Nkv0lHlxb9Q%3A2%3A1719888818%3A-

108. The first line of highlighted text again identifies Defendant's Pixel ID and confirms that it implemented the Pixel into its source code for this webpage and transmitted info to Facebook from this webpage.

109. The text ("GET"), at the top of the image, demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (highlighted as the c_user ID in the image above) thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.

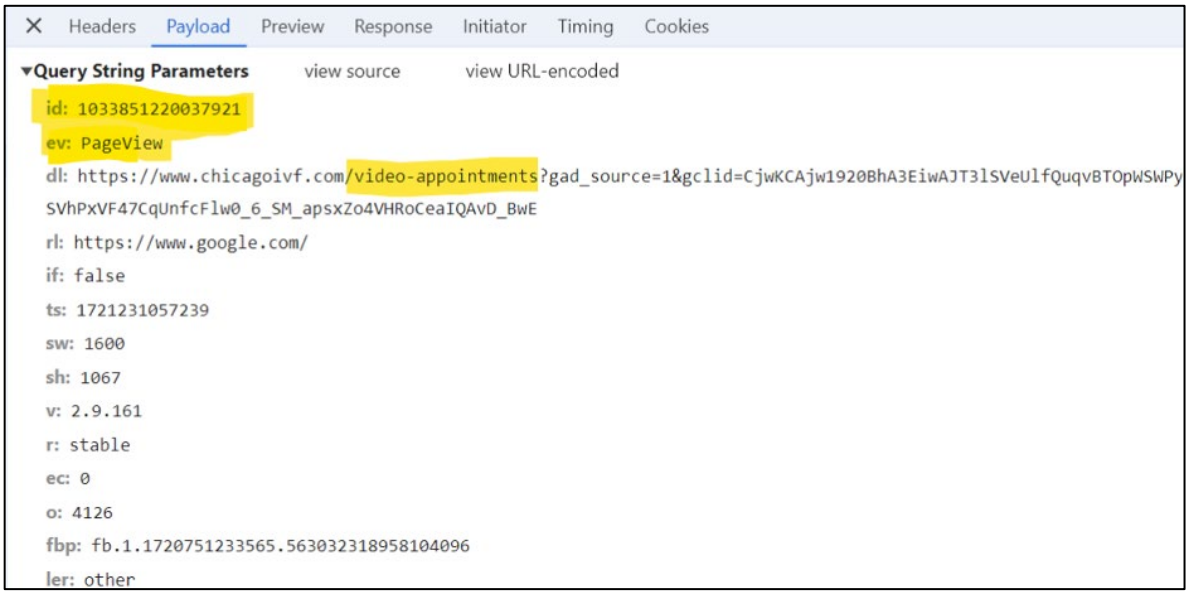
110. As Users move further into Chicago IVF's Website, Defendant continues to disclose User details through PageView events.

111. Defendant disclosed Users': (i) searches for specific doctors; (ii) fertility-related medical conditions; (iii) fertility treatments sought; (iv) patient status and (v) a user seeking an appointment.

112. For example, Defendant shares details about whether a User wants to set up a video appointment with a medical professional. When a User navigates to the "Video Appointments" page, Defendant sends PageView events revealing that the User was attempting to make a video appointment:[26]

[26] *See* https://www.chicagoivf.com/video-appointments (last visited Aug. 16, 2024).

Figure 4: Example of a HTTP single communication session sent from the User's device to Facebook that reveals the User was making a video appointment with Defendant



113. When a User searches for a doctor, Defendant also sends that information to Facebook through PageView events, including the specific doctor the patient is searching for.

114. Finally, when a User schedules a consultation for fertility treatment at one of Defendant's facilities, the details regarding that consultation, including the fertility treatment being performed by Defendant, is transmitted to Facebook.

Figure 5: Example of a HTTP single communication session sent from the User's device to Facebook that reveals the User was interested in scheduling a consultation for IUI treatment

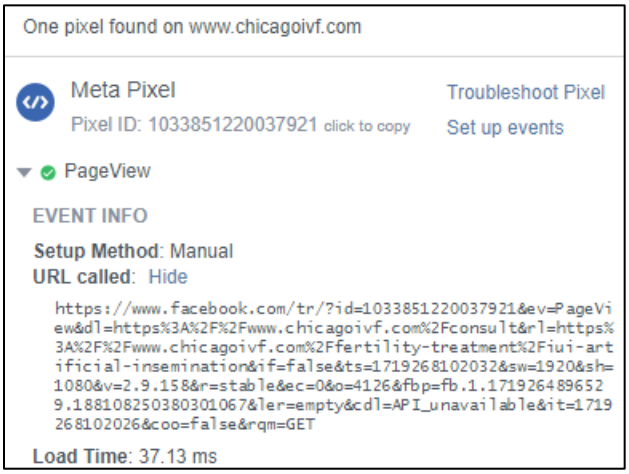
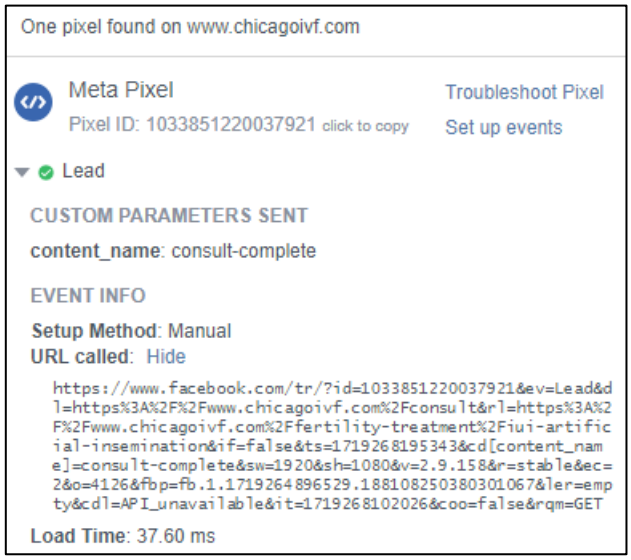


Figure 6: Example of a HTTP single communication session sent from the User's device to Facebook that reveals the User scheduled a consultation for IUI treatment



115. Specifically, a "Lead" event, as shown in Figure 6, indicates to Facebook that "a sign up is completed."[27]

116. In each of the examples above, the User's website activity and the contents of their communications are sent to Facebook alongside their PII. Several different methods allow marketers and third parties to identify individual Users, but the examples above demonstrate what happens when the website User is logged into Facebook on their web browser or device. When this happens, the Users' identity is revealed via third-party cookies that work in conjunction with the Pixels.

117. For example, the Pixel transmits the User's c_user cookie, which contains that User's unencrypted Facebook ID, and allows Facebook to link the User's online communications and interactions to their individual Facebook profile.

[27] META, https://developers.facebook.com/docs/meta-pixel/reference/

118. Facebook receives at least five cookies when Defendant's website transmits information via the Pixels, ***see*** **Figure 7:**

Name	Value	Domain	Path	Exp...	Size	Htt...	Sec...	Sa...
c_user	615605...	.facebook.com	/	202...	20		✓	None
datr	mGuD...	.facebook.com	/	202...	28	✓	✓	None
fr	1BSDA...	.facebook.com	/	202...	82	✓	✓	None
sb	mGuD...	.facebook.com	/	202...	26	✓	✓	None
xs	13%3A...	.facebook.com	/	202...	96	✓	✓	None

119. The fr cookie contains an encrypted Facebook ID and browser identifier.[28] Facebook, at a minimum, uses the fr cookie to identify Users, and this cookie can stay on a User's website browser for up to 90 days after the User has logged out of Facebook.[29]

120. At each stage, Defendant also utilizes the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a User.[30] ***See*** **Figure 8:**

Name	Value	Domain	Path	Exp...	Size	Htt...	Sec...	Sa...
_fbp	fb.1.17...	.chicagoivf.com	/	202...	41			Lax

121. The Pixel uses both first and third-party cookies, and both were used on the Website.[31]

[28] Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 23, 2024).

[29] Cookies & other storage technologies, https://www.facebook.com/policy/cookies/ (last visited May 23, 2024).

[30] The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

[31] A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. The _fbp cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the fr, _fbp, and c_user cookies to link website visitors' data to their Facebook IDs and corresponding accounts.

122. Defendant did not seek and did not have Plaintiffs' and Class Members' consent to share any of the sensitive Private Information described above.

D. Chicago IVF's Use of the Pixels Violated Its Own Privacy Policies.

123. Defendant's privacy policy represents to patients and visitors to its Website that it will keep their Personal Information, including their PHI, private and secure and that it will only disclose PHI provided to them under certain circumstances, ***none of which apply here***.[32]

124. With respect to tracking technologies and analytics, Defendant's privacy policy does not disclose to Users that it discloses their PHI and PII to third-parties, including Facebook.

125. For example, Defendant Chicago IVF's Policy admits that it collects information about its Users but that "we will not sell your health information or provide any of your health information to any outside marketing company."[33]

126. Defendant Chicago IVF's privacy policy does not acknowledge that it collects IP addresses, cookies, and similar technologies.[34]

127. Patients and other Users of the Website are not informed about and have not consented to the disclosure of their Personal Information and their Website activity to a third party, including Facebook.

128. This is precisely the type of information for which HIPAA requires healthcare providers to utilize de-identification techniques to protect the privacy of patients.[35]

---

[32] *See* https://www.chicagoivf.com/privacy-policy (last visited Aug. 16, 2024).

[33] *See Id*. (last visited Aug. 16, 2024).

[34] *Id*.

[35] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Feb. 2, 2024).

129. Despite a lack of disclosure, Defendant allows Facebook to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information that it promises to keep private.

130. Defendant breached its own privacy policies by unlawfully permitting Facebook and likely other third parties to intercept Users' Private Information without obtaining patients' consent or authorization. Facebook then read, understood, and used that Private Information for its own business purposes—i.e., selling targeted advertising to Defendant (and other companies) which specifically targeted those Users based on their reproductive health conditions.

E. Defendant Violated HIPAA.

131. Defendant's disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook also violated HIPAA.

132. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[36]

133. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

134. HIPAA's Privacy Rule defines "individually identifiable health information" ("IIHI") as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a

[36] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

135. The Privacy Rule broadly defines protected health information as IIHI that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

136. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (i) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'" or (ii) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

> A. Names;
> …
> H. Medical record numbers;
> …
> J. Account numbers;
> …
> M. Device identifiers and serial numbers;
> N. Web Universal Resource Locators (URLs);
> O. Internet Protocol (IP) address numbers; … and
> P. Any other unique identifying number, characteristic, or code… and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[37]

137. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

[37] *See* 45 C.F.R. § 160.514.

138. Even the fact that an individual is receiving a medical service, i.e., is a patient of a particular entity, can be PHI.

139. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[38]

140. Consistent with this restriction, HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[39]

141. Here, as described *supra*, Defendant provided patient information to third parties in violation of the Privacy Rule—and its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."

142. The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information … if the information is maintained by a covered entity

---

[38] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, (last visited Feb. 28, 2024).

[39] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Feb. 28, 2024).

… and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

143. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually identifiable health information relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

144. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306I, and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights," 45 C.F.R. § 164.312(a)(1)—which Defendant failed to do.

145. Under HIPAA, Defendant may not disclose PII about a patient, potential patient or household member of a patient for marketing purposes without the patient's express written authorization. See HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

146. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R. section 164.308(a)(6)(ii);

d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e) Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3); and

f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

147. In disclosing the content of Plaintiffs' and Class Members' communications, Defendant had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions, that is, to illegally disclose Plaintiffs' and Class Members' Private Information to Facebook (and other Pixel Information Recipients) in violation of HIPAA, including 42 U.S.C. § 1320d-6(a)(3), as well as the torts alleged below.

148. Defendant intercepted the content of Plaintiffs' and Class Members' communications, including their Private Information, for a criminal and tortious purpose. Defendant would not have been able to obtain the Private Information or the marketing services it did if it had complied with the law.

F. Users' Reasonable Expectation of Privacy.

149. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

150. Indeed, when Plaintiffs and Class Members provided their Personal Information to Defendant, they each had a reasonable expectation that the information would remain private, and

that Defendant would not share the Private Information with third parties for a commercial purpose unrelated to patient care.

151. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

152. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[40]

153. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

154. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as healthcare providers, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

[40] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Feb. 28, 2024).

G. Defendant was Enriched by & Benefitted from the Use of the Pixel & Other Tracking Technologies.

155. Defendant decided to embed the Pixel and other tracking technologies on its Website with the purpose of disclosing Plaintiffs' and Class Members's communications to Facebook and other Pixel Recipients in order to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Defendant and boost their revenue.

156. After receiving individually identifiable patient health information communicated on Defendant's Website, Facebook analyzes this data, improves its own technology and business (including machine learning), and then forwards this data and analysis of this data, to Defendant.

157. Defendant then uses this data and analysis for its own commercial purposes that include understanding how Users utilize its Website.

158. Facebook, as well, uses this data and analysis for its own commercial purposes, including to improve its platform and better understand the individuals that make up the audiences that its clients (advertisers) pay Facebook to target with ads.

159. Defendant also receives an additional commercial benefit from using Facebook's tracking tools, such as the Meta Pixel, in being able to serve more targeted advertisements to existing and prospective patients on their Meta accounts such as Facebook and Instagram.

160. Facebook advertises its Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting."[41]

[41] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Feb. 28, 2024).

161. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[42]

162. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendant's Website.

163. For example, when a User searches for doctors, medical conditions or treatment on Chicago IVF's Website, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a Chicago IVF ad and ensure that the targeted Users are more likely to convert.[43]

164. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[44]

165. Plaintiffs' and Class Members' Private Information has considerable value as highly monetizable data, especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

---

[42] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Feb. 28, 2024).

[43] *See, e.g.*, *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking (last visited Feb. 28, 2024).

[44] *Id*.

166. In exchange for disclosing the Private Information of their account holders and patients, Defendant is compensated by Facebook (and other Pixel Information Recipients) in the form of enhanced advertising services and more cost-efficient marketing on their platforms.

167. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[45]

168. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[46]

169. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[47]

170. Whether a user has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the pixels' ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where

---

[45] *See The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Feb. 28, 2024).

[46] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 90.

[47] *The complex world of healthcare retargeting, supra* note 89.

Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

171. Upon information and good faith belief, Defendant retargeted patients and potential patients, including Plaintiffs and Class Members.

172. Thus, utilizing the Pixels directly benefits Defendant by, among other things, reducing the cost of advertising and retargeting.

H. Plaintiffs' Private Information has Financial Value.

173. Plaintiffs' and Class Members' Private Information has value, and Defendant's disclosure and interception harmed Plaintiffs and Class Members by not compensating them for the value of their Private Information and, in turn, decreasing the value of their Private Information.

174. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

175. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

176. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[48] A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[49] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

---

[48] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Feb. 28, 2024).

[49] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Feb. 28, 2024).

177. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[50]That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

178. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[51]

179. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[52]

180. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

---

[50] *See What Your Data is Really Worth to Facebook* (July 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ (last visited Feb. 28, 2024).

[51] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

[52] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Feb. 28, 2024).

181. Courts recognize the value of personal information and the harm when it is disclosed without consent.[53]

182. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

183. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

184. The value of health data is well-known and various reports have been conducted to identify its value.

185. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[54]

---

[53] *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that Plaintiff's allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

[54] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Feb. 28, 2024).

186. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[55]

187. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[56]

188. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[57]

189. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

190. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

191. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

192. Defendant shared Plaintiffs' and Class Members' communications and transactions on its Website without permission.

---

[55] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Feb. 28, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[56] *See* https://time.com/4588104/medical-data-industry/ (last visited Feb. 28, 2024).

[57] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Feb. 28, 2024).

193. The unauthorized access to Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Website Users, including Plaintiffs and Class Members.

194. Plaintiffs have a continuing interest in ensuring that their future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

TOLLING

195. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its incorporation of the Meta Pixel into its website.

196. The Meta Pixel and other tracking tools on Defendant's website were and are entirely invisible to a website visitor.

197. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

198. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

199. Defendant had exclusive knowledge that its Website incorporated the Meta Pixel and other tracking tools and yet failed to disclose to customers, including Plaintiffs and Class Members, that by searching for and scheduling fertility treatment, Plaintiffs' and Class Members' Private Information would be disclosed or released to Meta and other unauthorized third parties.

200. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its customers' Private Information. In fact, to the present Defendant has not conceded, acknowledged, or otherwise indicated to its customers that it has disclosed or released their Private Information to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

201. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

202. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this Complaint.

203. Plaintiffs first discovered that Defendant had collected and shared their Private Information without her consent on or around August 2024 after contacting undersigned counsel and discussing potential claims against Defendant.

CLASS ACTION ALLEGATIONS

204. **Class Definition:** Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

205. The Nationwide Class that Plaintiffs seek to represent is defined as:

> All individuals residing in the United States who used Defendant's Website and had their Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

206. The Illinois Sub-Class that Plaintiffs seek to represent is defined as:

> All individuals residing in Illinois who used Defendant's Website and had their Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

207. Plaintiffs reserve the right to modify the class definition or add sub-classes as necessary prior to filing a motion for class certification.

208. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgment.

209. The Nationwide Class, and the Illinois Sub-Class are referred to collectively as the "Classes."

210. Excluded from the proposed Classes are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

211. Plaintiffs reserve the right to amend the definitions of the Class or Sub-class and add subclasses if further information and discovery indicate that the definitions should be narrowed, expanded or otherwise modified.

212. Numerosity/Ascertainability. Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiffs at this time. However, it is estimated that there are at least thousands of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records and non-party Facebook's records.

213. Typicality. Plaintiffs' claims are typical of the claims of the Classes because Plaintiffs used the Website and had their personally identifiable information and protected health information disclosed to Facebook without their express written authorization or knowledge. Plaintiffs' claims are based on the same legal theories as the claims of other Class Members.

214. Adequacy. Plaintiffs are fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the Class Members. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital

privacy litigation specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of the Classes.

215. Common Questions of Law and Fact. Questions of law and fact common to the Classes predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Classes:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. Whether Defendant had duties not to disclose Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant violated its privacy policies by disclosing Plaintiffs' and Class Members' Private Information to Facebook, Meta, or other third parties;

d. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been disclosed without their consent;

f. Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of patient's Private Information;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information;

h. Whether Defendant knowingly made false representations or omitted material representations as to their data security and/or privacy policy practices;

i. Whether Defendant knowingly omitted material representations with respect to their data security and/or privacy policy practices;

j. Whether Defendant's acts and practices violated Plaintiffs' and Class Members' privacy rights;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential or nominal damages as a result of Defendant's wrongful conduct; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

216. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class

action. Plaintiffs are unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1), *et seq.*
(On behalf of Plaintiffs & the Nationwide Class)

217. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and brings this count on behalf of themselves and the proposed Class.

218. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

219. The ECPA protects both sending and receipt of communications.

220. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

221. The transmissions of Plaintiffs' PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

222. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

223. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] ***any information concerning the substance, purport, or meaning of that communication***." 18 U.S.C. § 2510(8) (emphasis added).

224. Interception. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents . . . include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

225. Electronical, Mechanical, or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5).

226. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Defendant and Meta use to track Plaintiffs' and the Class Members' communications;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing devices;

d. Defendant's web-servers and

e. The Pixels deployed by Defendant to effectuate sending and acquiring Users' and patients' sensitive communications.

227. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Class Members' electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

228. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

229. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies it embedded and operated on its Website, contemporaneously and intentionally redirected and disclosed the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

230. Defendant's intercepted communications include, but are not limited to, the contents of communications to and/or from Plaintiffs' and Class Members' regarding PII and PHI, treatment, scheduling details and bill payments.

231. Additionally, through the above-described Tracking Technologies and intercepted communications, this information was, in turn, used by third parties, such as Facebook, to 1) place Plaintiffs in specific health-related categories based on their past, present and future health conditions and 2) target Plaintiffs with particular advertising associated with Plaintiffs' specific health conditions.

232. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while

knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

233. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

234. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Technologies to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

235. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

236. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Tracking Technologies.

237. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

238. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State, such as Illinois—namely, violations of HIPAA, among others.

239. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if

the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

240. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding and/or interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

241. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

242. Plaintiffs' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiffs' expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to intercept and then disclose Plaintiffs' and Class Members' PII and PHI for financial gain.

243. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

244. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed IIHI to Facebook and Google without patient authorization.

245. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook and Google source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

246. Healthcare patients have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Facebook Pixels and other tracking codes (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiffs' and Class Members' computing devices as "first-party" cookies that are not blocked.

247. The _fbp, ga, and cid cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

248. Defendant knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs' and Class Members' computing devices to remove, redirect, and disclose their data and the content of their communications with Defendant to Google, Facebook, and others.

249. Defendant's scheme or artifice to defraud in this action consists of: (a) the false and misleading statements and omissions in its privacy policy (HIPAA Notice) set forth above, including the statements and omissions recited in the claims below and (b) the placement of the

'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Meta.

250. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property rights (a) to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and (b) to determine who has access to their computing devices.

251. As such, Defendant cannot viably claim any exception to ECPA liability.

252. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their IIHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, treatments, and medical bills) for commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' IIHI without providing any value or benefit to Plaintiffs or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' IIHI, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;

d. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

253. As a result of Defendant's violation of the ECPA, Plaintiffs and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II

NEGLIGENCE
(On behalf of Plaintiffs & the Nationwide Class)

254. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and brings this count on behalf of themselves and the proposed Class.

255. Defendant owed Plaintiffs and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

256. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

257. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Technologies to disclose and transmit to third parties Plaintiffs' and Class Members' communications with Defendant, including Private

Information and the contents of such information.

258. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

259. The third-party recipients included, but may not be limited to, Facebook and/or Google.

260. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private

Information; and

i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

COUNT III

UNJUST ENRICHMENT
(On behalf of Plaintiffs & the Nationwide Class)

261. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and brings this count on behalf of themselves and the proposed Class.

262. This claim is pleaded in the alternative to Plaintiffs' other causes of action.

263. Defendant benefits from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at their expense.

264. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

265. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used and disclosed this information for its own gain including for advertisement purposes, sale or trade for valuable services from third parties.

266. Plaintiffs and Class Members would not have used Defendant's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

267. Defendant exceeded any authorization given and instead consciously disclosed and

used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

268. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

269. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

270. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

271. The benefits that Defendant derived from Plaintiffs and Class Members was not offered by Plaintiffs and Class Members gratuitously and rightly belongs to Plaintiffs and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

272. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT IV

Violation of the Illinois Eavesdropping Statute
720 ILCS § 5/14-1, *et seq.*
(On Behalf of Plaintiffs & the Illinois Subclass)

273. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set

forth herein and brings this count on behalf of themselves and the proposed Illinois Subclass.

274. The Illinois Eavesdropping Statute ("IES"), 720 ILCS § 5/14-1, et seq., prohibits the surreptitious interception, recording, or transcription of private electronic communications without the consent of all parties to the conversation and provides a civil cause of action to a person subjected to a violation of the IES against eavesdroppers and their principals.

275. Under 720 ILCS § 5/14-2(a)(3), the IES makes it unlawful for a person to knowingly and intentionally intercept, record, or transcribe, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication.

276. Under 720 ILCS § 5/14-2(a)(5), the IES makes it unlawful for a person to knowingly and intentionally use or disclose any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of the IES, unless he or she does so with the consent of all of the parties.

277. Under 720 ILCS § 5/14-2(a)(4), the IES makes it unlawful for a person to knowingly and intentionally "possesses any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious overhearing, transmitting, or recording of private conversations or the interception, or transcription of private electronic communications and the intended or actual use of the device is contrary to the provisions of" the IES.

278. The IES defines "private electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when

the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS § 5/14-1(e).

279. "Surreptitious," as used in the IES, "means obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS § 5/14-1(g).

280. An "eavesdropper" means "any person…who operates or participates in the operation of any eavesdropping device contrary to the provisions of [the IES] or who acts as a principal[.]" 720 ILCS § 5/14-1(b).

281. A "principal" includes any person who "[k]nowingly derives any benefit or information from the illegal use of an eavesdropping device by another" or "[d]irects another to use an eavesdropping device illegally on his or her behalf." 720 ILCS § 5/14-1(c).

282. An "eavesdropping device" is "any device capable of being used to…intercept…electronic communications[.]" 720 ILCS § 5/14-1(a).

283. Plaintiffs' communications with Defendant constituted private electronic communications. Plaintiffs transmitted their communications to Defendant from their computer or wire, intended the communications to be private, and reasonably expected the communications to be private under HIPAA, Defendant's express promises of confidentiality, the physician-patient relationship, and other State and federal laws protecting the confidentiality of Plaintiffs' communications.

284. Facebook and Google were not parties to Plaintiffs' private electronic communications with Defendant. Plaintiffs believed they were only communicating with Defendant, intended for their communications to be directed at Defendant only, and were unaware of the presence of concealed source code that redirected their communications.

285. Facebook and Google's interceptions of Plaintiffs' private electronic communications were knowing, intentional, and surreptitious. Facebook and Google intentionally designed their source code so that it could be concealed on websites to secretly intercept private communications. On information and belief, Facebook and Google knew that their source code was capable of, and in fact did, intercept private electronic communications without the consent of all parties to the communications.

286. Facebook and Google used and disclosed Plaintiffs' intercepted communications for advertising purposes.

287. Facebook and Google conduct was done without Plaintiffs' consent, in violation of 720 ILCS § 5/14-2(a)(3) and (a)(5).

288. Defendant acted as Facebook' and Google's "principal" under the IES. By deploying the source code from Facebook and Google on its Website, Defendant directed that Facebook and Google illegally eavesdrop on Plaintiffs' private electronic communications on its behalf and Defendant knowingly derived benefits and information from the illegal eavesdropping in the form of marketing.

289. Defendant further violated 720 ILCS § 5/14-2(a)(4) by possessing the source code, knowing that its design rendered it primarily useful for surreptitiously intercepting private electronic communications contrary to the IES.

290. Defendant' violation of the IES was wanton, reckless, and/or malicious.

291. For Defendant' violations of the IES, Plaintiffs and Class Members seek actual damages, punitive damages, injunctive relief, and any other relief the Court deems just.

RELIEF REQUESTED

292. Plaintiffs, on behalf of themselves and the proposed Class and Subclass,

respectfully request that the Court enter an order:

a. Certifying this action as a class action and appointment of Plaintiffs and Plaintiffs' counsel to represent the Class and Subclass defined above;

b. For equitable relief, enjoining Defendant from engaging in the unlawful practices and illegal acts described herein;

c. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

d. An award of damages, including but not limited to, (1) actual or statutory damages; (2) punitive damages in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorney fees and expenses and costs of suit; and (6) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Classes, demand a trial by jury for all claims asserted herein and so triable.

DATED: January 16, 2025

Respectfully submitted,

/s/ *Stephen A. Beck*

BURSOR & FISHER, P.A.
Sarah N. Westcot (*pro hac vice* forthcoming)
Stephen A. Beck
701 Brickell Avenue, Suite 2100
Miami, FL 33131
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: swestcot@bursor.com

sbeck@bursor.com

David S. Almeida (ARDC 6285557)
Matthew J. Langley (ARDC 6337129)
ALMEIDA LAW GROUP, LLC
Firm ID 100530
849 W. Webster Avenue
Chicago, Illinois 60614
Telephone: (312) 576-3024
Email: david@almeidalawgroup.com
matt@almeidalawgroup.com

HEDIN LLP
Frank S. Hedin (FBN: 109698)
1395 Brickell Ave, Suite 610
Miami, Florida 33131
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Attorneys for Plaintiffs & the Classes